UNITED STATES MARINE CORPS
MARINE CORPS LOGISTICS BASES
814 RADFORD BOULEVARD
ALBANY, GEORGIA 31704-0323

IN REPLY REFER TO:
2000
G600
APR 2 9 2002

POLICY STATEMENT 8-02

From: Commander
To: Distribution List

Subj: COMPUTER INCIDENT RESPONSE POLICY

Ref: (a) NAVSO P-5239-19 Computer Incident Response Guidebook
(b) OPNAVINST 2201.2 Navy and Marine Corps Computer Network Incident Response

Encl: (1) Virus Report Form
(2) Computer Incident Report Form

1. Purpose. To establish policy and procedures for the handling of computer incidents that will ensure quick and efficient recovery from these incidents. This policy, utilizing the guidance of references (a) and (b), will assist personnel in the protection of data, systems and personnel.

2. Background. Computer systems and the information they store are valuable resources that need to be protected. Increasingly sophisticated threats, including system and network intruders and computer viruses, can exploit a variety of weaknesses in computer systems and cause significant damage. Due to increased use of Local Area Networks (LANs), Intranets, and the Internet, damage caused by seemingly isolated computer security incidents can spread to other systems, causing widespread denial of service and other losses.

Steps need to be taken to understand the increased threats now affecting computer systems and learn how to respond to computer security incidents with the requisite speed and skill. This policy requires the use of Computer Emergency Response Teams (CERTs) as part of the MARCORLOGBASES Information Assurance (IA) program so that incidents can be contained and ultimately prevented in a timely and cost-effective manner.

Attacks against our computer systems could be an indication of, or associated with, an organized attack targeted against the entire Marine Corps Enterprise Network (MCEN). To identify and respond to such attacks, all Marine Corps Logistics Bases (MARCORLOGBASES) support personnel must work together to detect, protect and react to computer network attacks and threats. To support this effort, the MARCORLOGBASES G6 Information Assurance Office is the designated unit responsible for the coordination and reporting of all MARCORLOGBASES incidents to the Marine Corps Information Technology and Network Operations Center (MITNOC) and the Marine Forces Integrated Network Operations (MARFOR-INO).

3. Definitions

a. Computer network event: An event is any suspicious occurrence affecting an information system, (i.e. occasional port scan, bad Network Interface Card generating problems on the network, Intrusion Detection System thresholds set improperly thus generating false alarms).

b. Computer incident: An incident is any attempt to exploit or defeat the security features associated with a Marine Corps computer system such that the actual or potential adverse effects of the computer network attack may involve the compromise of information, loss or damage of property or information, or denial of service.

c. Types of incidents: The term "incident" encompasses the following general categories of adverse events:

(1) Malicious code attacks. Malicious code attacks include attacks by programs such as viruses, Trojan horse programs, worms, and scripts used by crackers/hackers to gain privileges, capture passwords, and/or modify audit logs to exclude unauthorized activity. Malicious code is particularly troublesome in that it is typically written to masquerade its presence and, thus, is often difficult to detect. Self-replicating malicious code such as viruses and worms can replicate rapidly, thereby making containment an especially difficult problem.

(2) Unauthorized access. Unauthorized access encompasses a range of incidents from improperly logging into a user's account (e.g., when a hacker logs in to a legitimate user's account) to unauthorized access to files and directories stored on a system or storage media by obtaining super user privileges. Unauthorized access could also entail access to network data by planting a "sniffer" program or device to capture all packets traversing the network at a particular point.

(3) Unauthorized utilization of services. It is not absolutely necessary to access another user's account to perpetrate an attack. An intruder can access information, plant Trojan horse programs, and so forth, by misusing available services. Examples include using the network file system to mount the file system of a remote server machine, a file access listener to transfer files without authorization, or inter-domain access mechanisms in Windows NT to access files and directories in another organization's domain.

(4) Disruption of service. Users rely on services provided by network and computing services. Perpetrators and malicious code can disrupt these services in many ways, including erasing a critical program, "mail spamming" (flooding a user account with electronic mail), and altering system functionality by installing a Trojan horse program.

(5) Misuse. Misuse occurs when someone uses a computing system for other than official purposes such as when a legitimate user uses a government computer to store personal tax records.

(6) Espionage. Espionage is stealing information to subvert the interests of the government. Many of the cases of unauthorized access to U.S. military systems during Operation Desert Shield/Desert Storm were espionage activities against the U.S. Government.

(7) Hoaxes. Hoaxes occur when false information about incidents or vulnerabilities is spread. In early 1995, for example, thousands of users with Internet access distributed information about a virus called the Good Times Virus, even though the virus did not exist. The vast majority of these users thought they were doing the right thing.

4. Reporting Procedures and Response Time

a. Virus Reporting Procedures:

(1) Base Level Information System Security Managers (ISSMs) will report incidents of computer viruses to the G6 Information Assurance Office within 24 hours of virus occurrence. If the virus has caused a widespread infection or is a new strain, the virus report will be forwarded to the G6 ISSM immediately. Reports will be submitted electronically using enclosure (1).

(2) The G6 Information Assurance Office will consolidate virus reports for MARCORLOGBASES and forward reports to the MITNOC, as required. If the virus has caused a widespread infection or is a new strain, the virus report will be forwarded to the MITNOC immediately upon receipt from the Base Level ISSM.

b. Other Computer Incident Reporting Procedures:

(1) The Base Level ISSMs will report computer incidents other than viruses to the G6 Information Assurance Office within 24 hours of occurrence. Reports will be submitted electronically using enclosure (2).

(2) If a system administrator suspects that a violation of law or policy has occurred, the matter should be reported to their chain of command. If the situation warrants an investigation, the commanding officer or supervisor should contact the local Naval Criminal Investigative Service or Provost Marshall Office (PMO) immediately. This will ensure that proper law enforcement investigation and evidence-handling procedures are adhered to for use at a criminal proceeding.

5. Actions

a. The Information Technology Department (AC/S, G6) has responsibility for providing command Information Technology (IT) leadership and guidance within MARCORLOGBASES. As such, the following AC/S, G6 actions apply to the MARCORLOGBASES CERT:

(1) Establish, review, update, publish and enforce command policy for computer incident response throughout MARCORLOGBASES

(2) Establish reporting and escalation procedures for computer incidents

(3) Forward incoming computer incident information from higher headquarters to the Base Level ISSMs in a timely fashion

(4) Coordinate incident response efforts within MARCORLOGBASES

(5) Conduct quarterly technical and functional reviews of MARCORLOGBASES incident response procedures for compliance with DoD, DoN, USMC, and command regulations

(6) Advise the Commanding General in the event of a serious computer incident

(7) Provide a monthly incident report summary to the MITNOC

b. The Local IT support sections, i.e., S6/Information Systems Office/Information Systems Management Office, will:

(1) Establish a local Computer Emergency Response Team - members of the CERT will be appointed in writing

(2) Prepare and distribute written incident procedures to all local users

(3) Ensure adequate training is provided to all users and Information Systems Coordinators (ISCs) to ensure familiarity with the command's local incident response procedures

(4) Provide incident reports as required to the MARCORLOGBASES G6 Information Assurance Office - reports will be submitted using enclosures (1) and (2)

(5) Provide users with a centralized POC for reporting all computer incidents

(6) Ensure audit trails and mechanisms are in place to identify any computer incidents that take place

(7) Create personnel recall rosters and provide communication equipment as needed to ensure personnel can be contacted 24 hours a day

(8) Establish and implement standard backup and recovery procedures

6. Administrative Actions. Failure to abide by this policy may result in administrative or punitive action. This may include loss of account access.

7. Point of Contact. Address questions concerning Information Assurance to MARCORLOGBASES AC/S, Information Technology Department, Information Assurance Office (G620) at DSN 567-7133 or Commercial (229)-639-7133. Email is matcomg6iaoffice@matcom.usmc.mil. Information can also be obtained from the MARCORLOGBASES G6 Information Assurance Office website at http://www.ala.usmc.mil/iao.

8. Applicability. This policy is applicable throughout all activities aboard MCLB Albany, MCLB Barstow, and Blount Island Command.

R.S. Kramlich
R. S. KRAMLICH

Distribution A

VIRUS REPORT
(Your Command name goes here…)

1. Name of infecting viruses:

2. Date viruses entered the command:

3. Major Source(s) of viruses:

4. Other locations, within or outside of the command, possibly infected as a result of these viruses:

5. Number and types of systems infected (i.e. hard disks and servers), along with the number of floppy diskettes infected:

6. Method of clean up:

7. Damage or observations resulting from the virus triggering:

8. Number of man-hours required in the effort:

9. Command POC:

COMPUTER INCIDENT REPORT
(Your Command name goes here…)

1. Report Date:

2. Incident Date:

3. Type of Incident:

4. Individuals Involved (name/office):

5. Cost of this Incident (downtime, cost, etc.):

6. Summary of Incident and Investigation Results (e.g., number of hosts attacked, how was access obtained, how was attack identified, was an Incident Response Organization contacted prior to submission of report, etc.)

7. Supervisors Recommendations/Comments:

8. Investigating Official:

9. Local Action to Prevent Reoccurrence:

10. Recommended Action by INFOSEC Official:

11. Attack Address:

12. Physical Location of System:

13. Hardware Configuration:

14. Operating System:

Enclosure (2)

COMPUTER INCIDENT REPORT
(Your Command name goes here…)

15. Security Software Installed:

16. Highest Level of Data Residing on System:

17. Damage or Observations Resulting from Attack:

18. Other Affected Hosts/Sites:

19. Your Command Name and Location:

20. Point of Contact at Your Command (i.e. ISSM - Include Commercial and DSN Phone Numbers)